UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/752,545	12/29/2000	Michael S. Ripley	42390P9905	1443

7590 05/04/2005

James Henry
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
HO, THOMAS M	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/752,545	RIPLEY, MICHAEL S.	
	Examiner	Art Unit	
	Thomas M. Ho	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *31-57* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *31-33,36-38,40-52 and 55-57* is/are rejected.

7)☒ Claim(s) *34, 35, 39, 53, 54* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment of 1/7/05 has been received and entered.

2. Claims 31-57 are pending.

Claim Objections

3. Claims 34, 35, 53, 54, 39 are objected to as being dependent on a rejected claim, but would have otherwise been allowable.

Response to Amendments

4. Applicant's arguments have been fully considered, but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 31, 32, 36, 37, 42-52, 55-57 are rejected under 35 U.S.C. 102(b) as being anticipated by Ishiguro et al., US patent 5883958.

In reference to claim 31:

Ishiguro et al. discloses a method comprising:

- formatting a media key block to include a column index record, where the media key block is the Key table which includes data in the form of records which may be indexed by column (Column index record) (Figure 7, "Key Table")
- and recording the media key block to a machine accessible medium, where the media key block is recorded to the DVD. (Figure 7, "Key Table")
- wherein the column index record comprises header information for two or more media key records, where the column index records include header information such as the ID fields. (Figure 7, "Key Table")
- and wherein the header information comprises column fields for two or more media key records, where the header information such as the ID information is a column field for the public key records and the encrypted encryption key records. (Figure 7, "Key Table")

In reference to claim 32:

Ishiguro et al. discloses a method according to claim 31 further comprising:

formatting the media key block to include both the column index record and a verify media key record within a single data transfer unit of the machine accessible medium, where the single data transfer unit is the track on the DVD. (Column 7, lines 27-33) & (Column 4, lines 6-15)

In reference to claim 36:

Ishiguro et al. discloses a method according to claim 31 Figure 7 & (Column 3, lines 14-22) wherein the machine accessible medium comprises a digital versatile disk (DvD-compliant medium.

In reference to claim 37:

Ishiguro et al. discloses a method according to claim 31 (Figure 7) wherein the operation of formatting the media key block to include a column index record comprises: arranging the column index record before a verify media key record in the media key block, where the column index record is the column which contains the IDs which is used to index the records, and the verify media key record is field in which the validity flags are kept (Column 4, lines 15-25), and Figure 7 displays the IDs to the left of or "before" the verify records.

In reference to claim 42:

Ishiguro et al. (Figure 7) discloses a method, comprising:

- reading a column index record from media key block stored on a machine accessible medium, wherein the column index record comprises header information for two or more media key records, and the header information comprises column fields for two or more media key records, where the column index record is the column of IDs which is also the header information in the key table, and the key table has more than one key record. (Figure 7)

- determining which of the two or more media key records should be accessed, based at least in pad on the column fields in the column index record for the two or more media key records, where the key is accessed and determined by using the ID field which is the column index record.

In reference to claim 43:

Ishiguro et al. (Figure 7) discloses a method according to claim 42, further comprising:

- accessing one or more of the media key records, based on the determination of which media key record should be accessed, where the media key records and determined and accessed via the Column of index records which is the IDs. (figure 9, S31-S32)
- calculating a media key, based at least in part on information obtained from the accessed media key record, where the information obtained from the accessed media key is used to compute the encrypted media key (Figure 9, S32 – Figure 9, S37)

In reference to claim 44:

Ishiguro et al. (Figure 7) discloses a method according to claim 42, further comprising:

- accessing one or more of the media key records, based on the determination of which media key record should be accessed, wherein the operation of accessing one or more of the media key records is performed by a device having a predetermined column value; (Figure 9, S31-S33)
- wherein the operation of accessing one or more of the media key records comprises accessing media key records that include encrypted key data fields only if those media

key records comprise a column value that corresponds to the predetermined column value for the device, where the column value is the IDs (Figure 7)

Claims 45-47 are substantially similar to claims 42-44 and are rejected for the same reasons.

Claim 48 is rejected for the same reasons as claim 43.

In reference to claim 49:

Ishiguro et al. (Figure 7) discloses n apparatus according to claim 45, wherein the apparatus comprises a data processing system, where the data processing system processes DVD data.

Claims 50-51 are substantially similar to claims 31-32 and are rejected for the same reasons.

In reference to claim 52:

Ishiguro et al. (Figure 7) discloses an apparatus according to claim 50, wherein: the media key block comprises multiple media key records with encrypted key data fields; and each encrypted key data field resides completely within a single data transfer unit of the machine accessible medium, where the encrypted data field resides in the key block, and the key block in a single data transfer unit, the DVD track.

Claims 55-56 are rejected for the same reasons as 36-37.

In reference to claim 57:

Ishiguro (Figure 9, S32 – Figure 9, S37) & (Figure 11, Item 72) discloses an apparatus according to claim 50, wherein:

- the machine accessible medium further comprises encrypted content, where the machine accessible medium has encrypted keys and DVD content. (Figure 11, Item 72)
- and at least one of the media key records comprises data that may be used to calculate a media key for decrypting the encrypted content. (Figure 9, S32 – Figure 9, S37)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claim 33, 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al.

Claims 40, 41 are rejected 35 U.S.C. 103(a) as being unpatentable over Ishiguro et al. and Lotspiech., US patent 6609116.

In reference to claim 33:

Ishiguro et al. fails to disclose a method according to claim 32, wherein the single data transfer unit comprises an error control code (ECC) block.

The Examiner takes official notice however that transferring information as a single unit as an ECC block was well known in the art at the time of invention. The ECC block for DVDs is set in the ECMA standard for 120mm DVDs as having 16 consecutive frames in an array of 192 rows of 172 bytes each. Indeed, the Applicant recites that this limitation is known and has placed it in the background of the invention. (Specification, page 4, lines 10-15).

It would have been obvious to one of ordinary skill in the art at the time of invention to have a single data transfer *comprise* an ECC block (32768 bytes) in order to conform to current DVD specifications.

In reference to claim 38:

Ishiguro et al. fails to discloses a method according to claim 31 appending sufficient filler bytes to a first media key record within the media key block to cause an encrypted key data field of a subsequent media key record to be positioned completely within a single data transfer unit of the machine accessible medium. (Column 7, lines 27-33) & (Column 4, lines 6-15)

Ishiguro et al. discloses a first media key record within the media key block with an encrypted data key that is positioned completely within a single data transfer unit of the machine accessible medium, where the single data unit is the DVD track.

It is of note that in Ishiguro, while the mechanism for the positioning subsequent key records is not stated, it is evident that subsequent key records are positioned properly. For Example, figure 5, has ID#2 positioned against the field contained ID#1 subsequent to that field.

The Examiner takes official notice that using filler bytes as a mechanism to adjust the length of a data field to fit the rest of block of information is well known in the art.

For Example, spreadsheets will often add multiple zeros as a place holder in particular column so that numbers align. Money also uses filler bytes to allow a number to be positioned completed. For example $1.04 uses the zero as a place holder.
Filler bytes are also appended to tracks of the CD, usually as a string of zeros, to fill up unused portions of a CD or DVD.
Such positioning is performed as a matter of formatting to make reading and understanding easier.

It would have been obvious to one of ordinary skill in the art at the time of invention to append sufficient filler bytes to a media key record to cause a subsequent media key record to be positioned completely together, within the data track in order to better organize the key information to make reading and understanding easier.

In reference to claim 40:

Ishiguro et al. fails to disclose a method wherein the subsequent media key record with the encrypted key data field to be positioned completely within the single data transfer unit comprises a calculate media key record (CMKR).

Lotspiech discloses a media key block that is generated through CMKR command. (Column 2, lines 13-25) where the CMKR command is a command to "calculate a media key" block or record.

Lotspiech discloses (Column 1,line 60- Column 2, line 25) that the ability to calculate the media key record allows new media key blocks to be produced avoiding any suspected compromised media key blocks.

Ishiguro Figure 9, discloses computing specialized encryption keys from the old media key block, where this block is on the single data unit of a track. (Column 7, lines 27-33) & (Column 4, lines 6-15)

It would have been obvious to one of ordinary skill in the art at the time of invention to use the CMKR to derive a media key block from an old one (a subsequent media key record) in order to increase security and avoid using suspected media key blocks.

In reference to claim 41:

Ishiguro et al. fails to disclose a method wherein the subsequent media key record with the encrypted key data field to be positioned completely within the single data transfer unit comprises a conditionally calculate media key record (CCMKR).

Lotspiech discloses a media key block that is generated through CCMKR command. (Column 5, lines 35-45) where the CCMKR command is a command to "conditionally calculate a media key" block or record.

Lotspiech discloses (Column 1,line 60- Column 2, line 25) that the ability to calculate the media key record allows new media key blocks to be produced avoiding any suspected compromised media key blocks.

Ishiguro Figure 9, discloses computing specialized encryption keys from the old media key block, where this block is on the single data unit of a track. (Column 7, lines 27-33) & (Column 4, lines 6-15)

It would have been obvious to one of ordinary skill in the art at the time of invention to use the CCMKR to derive a media key block from an old one (a subsequent media key record) in order to increase security and avoid using suspected media key blocks.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of the final action and the advisory action is not mailed under after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension pursuant to 37 CFR 1.136(A) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

Customer Service Representative Telephone: 571-272-2100 Fax: 703-872-9306

TMH

April 30th, 2005